IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC, ***Plaintiff,*** v. **FUJITSU LTD.; FUJITSU AMERICA, INC.; AND SAP AMERICA, INC.,** ***Defendants.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Marking Object Virtualization Intelligence, LLC ("MOV Intelligence" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,200,230 ("the '230 patent"); 6,802,006 ("the '006 patent"); 6,510,516 ("the '516 patent"); 7,650,504 ("the '504 patent"); and 7,124,114 ("the '114 patent") (collectively, the "patents-in-suit" or the "MOV Intelligence Patents"). Defendants Fujitsu Ltd.; Fujitsu America, Inc. (collectively, "Fujitsu") infringes the '230, '006, '504, and '114 patents. Defendants Fujitsu and SAP America, Inc. ("SAP") (Fujitsu and SAP, collectively, "Defendants") jointly infringe the '516 patent. Defendants infringement violates the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.*

INTRODUCTION

1. Rovi Corporation ("Rovi") is a pioneer and leader in protecting computer technology, including digital rights management ("DRM") and digital watermarking systems. In 1985, Rovi, then known as Macrovision Corporation ("Macrovision"), introduced the first system for protecting digital content on VHS tapes.[1] By 2001, Rovi's Macrovision technology

[1] Aljean Harmetz, *Cotton Club Cassettes Coded to Foil Pirates*, N.Y. TIMES (April 24, 1985) ("The device, which works by confusing a recorder's automatic gain control - the mechanism that controls the strength of the signal on the tape - was demonstrated at a news conference today by its inventor, John Ryan of Macrovision.").

was ubiquitous in the distribution of video content and employed in 75% of DVDs sold in the United States.[2] In the late 1990's, Rovi applied its video copy protection expertise to DRM and encryption for operating systems and executable files. Rovi developed groundbreaking products including: Macrosafe; SafeDisc; FlexLm; SafeAuthenticate; SafeCast; and InstallShield.

2. To facilitate the licensing of Rovi's foundational technology, including U.S. Patent Nos. 6,802,006 and 6,510,516, Rovi licensed and/or assigned 233 of its foundational patents to MOV Intelligence. Rovi assigned MOV Intelligence many of John O. Ryan's, the founder of Rovi predecessor Macrovision, groundbreaking patents.[3] MOV Intelligence owns, protects and licenses Rovi's inventions to allow companies to operate in the marketplace and ensure Rovi's labor and ingenuity is fairly compensated.

THE PARTIES

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC

3. Marking Object Virtualization Intelligence, LLC ("MOV Intelligence") is a Texas limited liability company with its principal place of business located at 903 East 18th Street, Suite 217, Plano, Texas 75074. MOV Intelligence is committed to advancing the current state of DRM and watermarking technologies.

4. MOV Intelligence Global Licensing, LLC ("MOV Global Licensing") is a wholly-owned subsidiary of MOV Intelligence and assists in the licensing of MOV Intelligence's patents in territories outside the United States with a focus on the European Union (and the United Kingdom).[4] MOV Intelligence Global Licensing, LLC is a corporation organized under the laws of Delaware.

---

[2] Eileen Fitzpatrick, *Picture This*, BILLBOARD MAGAZINE at 59 (March 24, 2001) ("[Macrovision] provides its technology to 75% of all DVDs distributed by Hollywood studios. Overall, the company has copy-protected more than 800 million DVDs, 8 billion videocassettes and 45 million digital set-top boxes.").

[3] *See* U.S. Patent Nos. 6,381,367; 7,764,790; 6,701,062; 8,014,524; German Patent Nos. DE60001837 and DE60001837D1; Chinese Patent No. CN1186941C; Canadian Patent No. CA2379992C; European Patent No. EP1198959B1; and Japanese Patent No. JP4387627B2.

[4] Wolfram Schrag, *EU-Patent steht auf der Kippe*, BR.COM NACHRICHTEN (August 2016).

5. In an effort to obtain compensation for Rovi's pioneering work in the fields of copy protection and digital security, Rovi assigned the following patents to MOV Intelligence: U.S. Patent Nos. 7,299,209; 6,510,516; 6,802,006; 7,650,504; 6,813,640; 7,650,418; 7,200,230; 7,124,114; 6,381,367; 6,374,036; 6,360,000; 6,553,127; 6,701,062; 6,594,441; 7,764,790; 8,014,524; 6,931,536; and International Patent Nos. DE60047794; DE60148635.8; DE60211372.5; DE69901231.7-08; DK1047992; EP1047992; EP1303802; EP1332618; EP1444561; ES1047992; FR1047992; FR1303802; FR1332618; FR1444561; GB1047992; GB1303802; GB1332618; GB1444561; GR3040059; IE1047992; IE1444561; IT1047992; NL1047992; NL1444561; PT1047992; and SE1047992.

6. In a further effort to help protect Rovi's trailblazing technology, Rovi appointed MOV Intelligence as an authorized licensing agent for the following international patent assets: AT1020077; AT1198959; AT1080584; ATE232346; AT1020077; AU729762; AU741281; AU753421; AU743639; AU714103; AU729762; AU2002351508; AU765747; AU2000263715; BE1020077; BE1198959; BE1020077; BE1080584; BE900498; BRPI 9812908-2; BR9709332.7; BRPI 9812908-2; CA2305254; CA2332546; CA2379992; CA2305254; CA2332548; CA2557859; CA2252726; CA2462679; CA2315212; CA2416304; CA2425115; CH1020077; CH1080584; CH900498; CH1020077; CH1047992; CNZL98809610.2; CNZL99806376.2; CNZL00811179.0; CNZL98809610.2; CNZL99806377.0; CNZL97194746.5; CNZL02820738.6; CNZL99802008.7; CNZL00819775.X; CNZL200510089437; DE69807102.608; DE60001837.7; DE69908352.4-08; DE69718907.4-08; DE69807102.608; DK1020077; DK1080584; DK1198959; DK1020077; DK900498; EP1020077; EP1198959; EP1080584; EP900498; EP1020077; ES1020077; ES1198959; ES1080584; ESES2191844; ES1020077; FI1020077; FI1080584; FI1020077; FI900498; FR1020077; FR1198959; FR1080584; FR900498; FR1020077; GB1020077; GB1198959; GB1080584; GB900498; GB1020077; GR3041381; GR3045620; GR3043304; GR3041381; HK1028696; HKHK1035625; HK1028696; HK1035282; HK1018562; HKHK1069234; HKHK1057115; HK1083653B; IE1020077; IE1198959; IE1020077; IE1080584; IE900498;

IL135498; IL139543; IL148002; IL135498; IL139544; IN201442; IN220504; IN201442; IN207829; IT1020077; IT1080584; IT900498; IT1020077; JP4139560; JP4263706; JP4387627; JP4551617; JP4139560; JP4263706; JP3542557; JP4627809; JP4698925; JP4366037; JP4307069; KR374920; KR422997; KR761230; KR374920; KR362801; KR478072; KR689648; KR539987; KR752067; KR728517; KR593239; MX223464; MX231725; MX226464; MX223464; MX212991; MX214637; MX237690; MX240845; MYMY-123159-A; MYMY-123159-A; NL1020077; NL1198959; NL1080584; NL900498; NL1020077; NZ503280; NZ507789; NZ503280; NZ532122; PT1010077; PT1198959; PT1080584; PT900498; PT1010077; RU2195084; RU2216121; RU2251821; RU2195084; RU2208301; RU2258252; SE1020077; SE1198959; SE1080584; SE900498; SE1020077; SG71485; SG76965; SG86547; SG76964; SG71485; TWNI117461; TWNI-124303; TWNI-130428; TWNI1600674; TWNI-162661; TWNI-202640; TWNI117461; TWNI-130754; and TWNI-184111.

7. MOV Intelligence and its wholly-owned subsidiary, MOV Global Licensing, pursues the reasonable royalties owed for Defendants' use of Rovi's groundbreaking technology both here in the United States and throughout Europe. Rovi maintains 7,500 square feet of office in Plano, Texas. Rovi maintains off-site document storage at Plano, Texas, where Rovi stores over 4,800 boxes of hard-copy documents, at least some of which are relevant to this case. Rovi also maintains a datacenter located in Allen, Texas, where at least some email, source code and software relating to the patents-in-suit in this action are stored.

FUJITSU LTD.

8. On information and belief, Fujitsu, Ltd. is a Japanese corporation with its principal place of business at Shiodome City Center, 152 Higashi-Shimbashi, Minato-ku, Tokyo 105-7123, Japan.

FUJITSU AMERICA, INC.

9. On information and belief, Fujitsu America, Inc. is a California corporation with its principal place of business at 1250 East Arques Avenue, Sunnyvale, California 94085. Fujitsu America, Inc. may be served through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. On information and belief, Fujitsu America, Inc. is registered to do business in the State of Texas, and has been since at least November 7, 2000.

10. On information and belief, Fujitsu America, Inc. conducts business operations throughout the State of Texas.

SAP AMERICA, INC.

11. On information and belief, SAP America, Inc. is a Delaware corporation with its principal place of business at 3999 West Chester Pike, Newtown Square, Pennsylvania 19073. SAP may be served through its registered agent CT Corporation System 1999 Bryan Street, Suite 900, Dallas, Texas 75201. On information and belief, SAP is registered to do business in the State of Texas, and has been since at least June 15, 1992.

12. On information and belief, SAP conducts business operations throughout the State of Texas, including at its facilities at 5212 N. O'Connor Boulevard, Suite 800, Irving, Texas 75039, and 2601 Westheimer Road, Suite C250 Houston, Texas 77098.

THE FUJITSU-SAP JOINT SOLUTION

13. On information and belief, Fujitsu and SAP, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the PRIMEFLEX for SAP HANA and PRIMEFLEX for SAP Landscapes (collectively, "PRIMEFLEX for SAP HANA"). SAP and Fujitsu describe PRIMEFLEX for SAP HANA as being an "integrated" "all-in-one package."

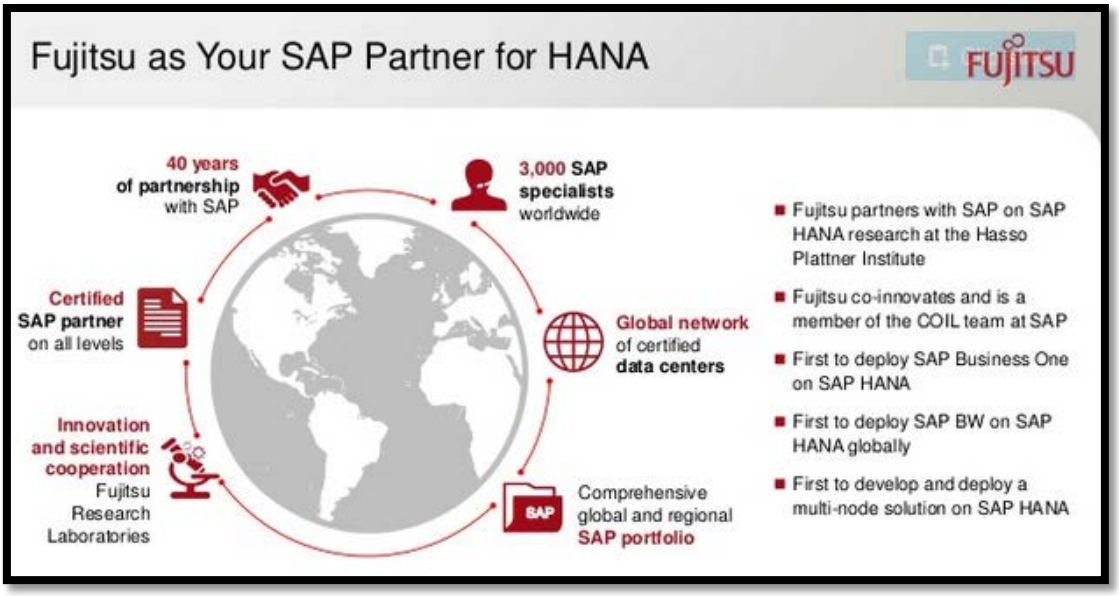
> Integrated systems can simplify the implementation and operation of SAP environments. That's why Fujitsu's PRIMEFLEX for SAP Landscapes and PRIMEFLEX for SAP HANA are pre-defined and pre-tested infrastructure solutions, ***coming as all-in-one packages*** which combine servers, storage, network connectivity and software.

Fujitsu Solutions for SAP Environments, FUJITSU.COM WEBSITE (last visited September 2016), available at: http://www.fujitsu.com/us/solutions/infrastructure/dynamic-infrastructure/

14. Fujitsu and SAP offer the PRIMEFLEX for SAP joint solution based on contractual agreements between SAP and Fujitsu. Rainer Hettingerof the Global Fujitsu SAP Competence Center described the PRIMEFLEX for SAP product as an "integrated system."

Rainer Hettinger, *Next Generation SAP Landscape Based on SAP HANA - Smooth Transformation Enabled by Fujitsu Solutions and Services*, FUJITSU WORLD TOUR 2015 PRESENTATION (2015), available at https://www.youtube.com/watch?v=mP3T4_3Mi-s ("we are a partner of SAP for more than forty years . . . and we are since then not only a technology partner but also a service partner, hosting, and cloud partner. . . . And we support globally more than 10,000 customers.").

15. Further, Fujitsu and SAP have jointly developed the PRIMEFLEX for SAP HANA joint solution by partnering on research at the Hasso Plattner Institute, Fujitsu serving as a member of the SAP Co-Innovation Lab ("COIL"), and jointly selling the PRIMEFLEX for SAP HANA joint solution.



Fujitsu: Your Partner for SAP HANA Solutions, FUJITSU AMERICA PRESENTATION at 4 (March 9, 2016).

16. Defendants have described the PRIMEFLEX for SAP HANA as being "designed holistically."[5] Further the PRIMEFLEX for SAP HANA systems is described as containing "[s]ervers, storage, network connectivity and software [that] are pre-integrated and perfectly harmonized. The infrastructure is completely set up in the Fujitsu Staging Center, where it is also tested before delivery to the customer as a ready-to-run solution."[6]

17. The PRIMEFLEX for SAP HANA joint solution has been described by Fujitsu in industry publications as and "end-to-end" solution that "seamlessly" integrates PRIMEFLEX with SAP HANA.

> Fujitsu PRIMEFLEX for SAP HANA is a pre-defined and pre-tested infrastructure solution based on SAP-certified components that enables simplified, fast, and secure implementation and operation of the SAP HANA platform. This solution can be seamlessly integrated with Fujitsu PRIMEFLEX for SAP landscapes, which provides a unique operational concept for effectively running SAP applications and databases in businesses of all sizes and in all types of industries. . . . By properly orchestrating and automating failover processes, Fujitsu's FlexFrame Orchestrator software, a core component of PRIMEFLEX for

[5] *Simplify SAP Operations: Fujitsu Integrated System PRIMEFLEX for SAP Landscapes*, FUJITSU WHITEPAPER at 4 (2015).
[6] *Id.*

> SAP landscapes, provides the basis for effective high availability and disaster recovery (DR).

Andrea Voigt and Paul Mantey, *Balance Credibility and Costs*, SAPINSIDER SPECIAL REPORT: TAKING THE NEXT STEP WITH SAP HANA at S-9 (April 1, 2015) (Andrea Voigt is the Senior Product Marketing Manager at Fujitsu Global Marketing Services and Solutions).

18. As described in Count III, below, Defendants' PRIMEFLEX for SAP HANA joint solution infringes the '516 patent. Defendants are properly joined in this action pursuant to 35 U.S.C. § 299.

JURISDICTION AND VENUE

19. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

20. Upon information and belief, this Court has personal jurisdiction over Defendants in this action because Defendants have committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. Defendants, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. In addition, Fujitsu America, Inc. and SAP are registered to do business in the State of Texas.

21. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Fujitsu America, Inc. and SAP are registered to do business in Texas, and upon information and belief, all Defendants have transacted business in the Eastern District of Texas and have committed acts of direct and indirect infringement in the Eastern District of Texas.

MOV INTELLIGENCE'S LANDMARK INVENTIONS

22. The groundbreaking inventions in DRM and digital watermarking taught in the patents-in-suit were pioneered by Rovi. Respect for intellectual property is at the center of

Rovi's business. Rovi, first established in 1983 under the name Macrovision, is a trailblazing technology company initially focused on inventing and bringing to market fundamental technologies designed to allow producers and distributors of film and music to widely distribute their products while simultaneously protecting their art from unauthorized copying.

23. In 1985, Rovi introduced the first copy protection for VHS tapes. The Macrovision copy protection system took advantage of the NTSC video standard being defined by a 525-line vertical resolution. However, only 480 of those lines are used for transmitting video information. The extra 45 lines were used to carry control codes such as interlace information, closed captions, and other similar non-video content. The Macrovision copy protection system worked by adding certain codes to these control lines that were interpreted by an Automatic Gain Control chip in a VCR to scramble the video signal if it was being recorded. The film "Cotton Club" was the first to incorporate the Macrovision copy protection technology.

The New York Times

April 24, 1985

'COTTON CLUB' CASSETTES CODED TO FOIL PIRATES

By ALJEAN HARMETZ

HOLLYWOOD, April 23— When video cassettes of "The Cotton Club" go on sale Wednesday, they will be coded with a new antipiracy device designed to keep America's 20 million video-cassette recorder owners from making copies for their friends. The device is also aimed at deterring the operators of the country's 15,000 video-cassette stores from buying a single copy of a movie and then making an extra dozen copies to rent out.

Aljean Harmetz, *Cotton Club Cassettes Coded to Foil Pirates*, N.Y. TIMES (April 24, 1985).

24. Macrovision's copy protection technology became ubiquitous in the motion picture industry. By 2001, 75% of DVDs sold in the United States incorporated Macrovision's copy protection technology. Macrovision's copy protection technology became so important to content creators that Congress specifically regulated the manufacture and sale of technology that was incompatible with Macrovision's copy protection technology. In the Digital Millennium Copyright Act, Congress outlawed VHS technology incompatible with Macrovision's automatic

gain control copy control technology. *See* 17 U.S.C. § 1201(k)(1) ("unless such recorder conforms to the automatic gain control copy control technology").[7]

25. Rovi broadened its focus on video scrambling technologies to include copy protection and DRM for other media, including computer executables, firmware, operating system images, watermarking, and encryption. The company's products, including "MacroSafe," "SafeDisc," "FLEXlm," "FLEXnet," "SafeAuthenticate," "SafeCast," "SafeWrap," "SAM Solutions," and "GT Licensing" were broadly adopted by technology companies.

26. As media technology advanced over the decades from VHS to DVD to digital files hosted and served over the Internet and in the cloud, Macrovision kept pace, inventing industry-leading copy protection and digital security solutions that ensured content creators' intellectual property was protected. Macrovision developed breakthrough technologies, including "SafeDisc," a technology directed at preventing professional pirating by thwarting attempts to use CD-recordable drives or hard discs to make useable copies of CD-ROMs.

CD Protection May Be Ready For Takeoff

Macrovision Thinks Legit Downloads Could Spur Use Of Anti-Piracy Technology

BY CATHERINE APPLEFELD OLSON

CD copy-protection technology company Macrovision hopes that the out-of-the-box popularity of Apple's iTunes pay-per-download music store, coupled with the rise of similar services, may help spur label adoption of anti-piracy technology on physical goods.

"We are entering a new phase; the whole game is going to change," says Adam Sexton, VP of marketing for Macrovision's music technology division. "Until now, there has not really been a good, legit alternative for music fans. Napster showed us the demand was there, and now, in the post-iTunes world, with others planning to offer these new kinds of services, consumers do have good options online."

SEXTON

While record companies are actively discouraging file trading on peer-to-peer (P2P) networks, Sexton argues that they need to remember that "right now, every unprotected CD is a perfect source to pollute those P2P networks."

PICKING UP STEAM

With a licensing agreement with Microsoft in place and young digital services to protect, Santa Clara, Calif.-based Macrovision believes it is poised to accelerate the use of CD copy protection in the U.S.

The company is still eyeing fourth-quarter 2003 for at least one general-market trial here.

"This summer will be very telling," Sexton predicts. "We are presenting the new combined

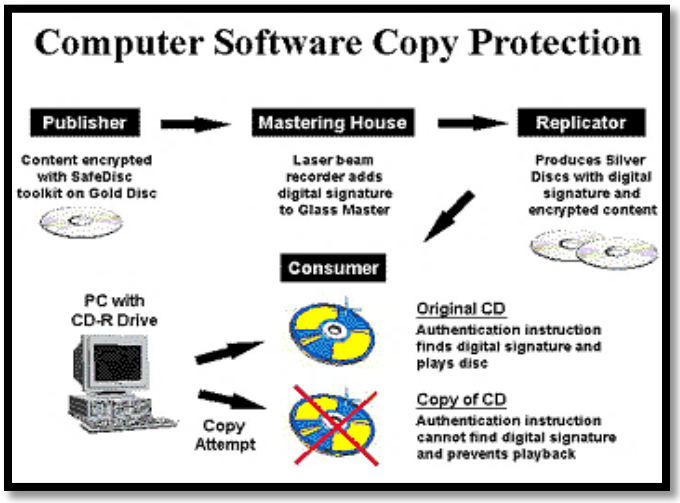
(Continued on page 57)

Catherine Applefeld Olson, *CD Protection May Be Ready for Takeoff*, BILLBOARD MAGAZINE at 55 (June 28, 2003).

27. SafeDisc was one of Rovi's groundbreaking DRM products. SafeDisc authenticated computer image files using authenticating digital signatures embedded on an executable disc, as well as a multi-layered encrypted wrapper that secured the executable content. The SafeDisc digital signature, which could not be copied by recorders or mastering

[7] *See also* David Nimmer, *Back from the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 862 (2001) (The DMCA "contains a welter of corporation-specific features, relating to Macrovision Corp. The features in question relate to section 1201's controls on consumer analog devices.") (citations omitted).

equipment, was embedded via a laser beam recorder at the time the disc master was produced at a mastering facility. In its first sixty days of production, Rovi's SafeDisc technology was applied to over one million computer programs and licensed to seventeen mastering and replication facilities worldwide. Shortly after its introduction, Rovi's SafeDisc technology was incorporated in thirty-two products, including products from GT Interactive, Interplay, Microprose, Red Storm Entertainment, Take 2 Interactive Software, and TalonSoft.

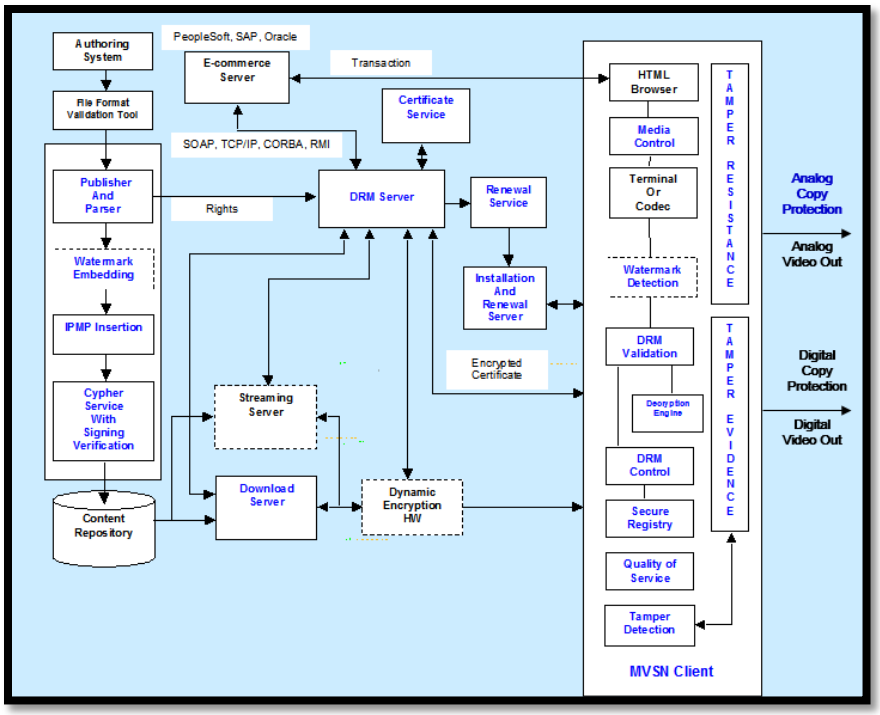


Rovi SafeDisc Copy Protection Overview, MACROVISION CORPORATION DATASHEET at 2 (1999) ("SafeDisc incorporates a unique authentication technology that prevents the re-mastering of CD-ROM titles and deters attempts to make unauthorized copies. The SafeDisc authentication process ensures that consumers will only be able to play original discs. The user is forced to purchase a legitimate copy.").

28. When users inserted a Rovi SafeDisc protected disc containing executable software in a drive, the authentication software verified the digital signature, allowing the program to be decrypted and run normally. If an unauthorized copy was loaded, the authentication software would be unable to authenticate the digital signature, and the executable would not run. Subsequent versions of SafeDisc (Version 2.0, released September 2000; Version 3.0, released 2003; and Version 4.0, released 2004) incorporated additional groundbreaking DRM functionality including digital signature authentication, unique signature files for each protected work, and support for 128-bit encryption. An important feature of SafeDisc was the multi-level, anti-hacking technology that prevented the compromise of security features. The

Rovi SafeDisc technology was designed to not only deter consumer copying, but to also thwart experienced commercial pirates.

29. Rovi's MacroSafe was another trailblazing digital rights management technology developed by Macrovision. MacroSafe was a multi-layered software solution for the secure distribution and management of video, audio, graphics, and other multimedia applications for PCs, as well as for a variety of non-PC devices including set-top boxes, PDAs, portable entertainment devices, and digital consumer electronics appliances. Released in 2002, MacroSafe introduced 192-bit, AES encryption coupled with a key escrow server that enabled the secure distribution of digital content. The below high-level schematic shows the architecture of the MacroSafe system.



Kirby Kish, MACROSAFE SYSTEM: A SOLUTION FOR SECURE DIGITAL MEDIA DISTRIBUTION at 7 (January 2002) (showing the architecture of the MacroSafe system and use of a DRM Server and Key Escrow Server).[8]

[8] *See also* Michael Arnold et al., TECHNIQUES AND APPLICATIONS OF DIGITAL WATERMARKING AND CONTENT PROTECTION 203 (2002) (Describing Rovi's Cactus Data Shield product which by 2002 had been used in over 100 million compact discs. "This scheme [Rovi Cactus Data Shield] operates by inserting illegal data values instead of error-correcting codes.").

30. To maintain Rovi's leadership position in the industry, Rovi invested and continues to invest significant resources in the design, development, and licensing of its copy protection products and related technologies. Since 2013 alone, Rovi has invested over $300 million dollars in research and development. Furthermore, Rovi employs close to 800 full-time workers throughout the United States, including at Rovi's Plano, Texas office.

31. The importance of Rovi's innovate solutions has been recognized by numerous leading industry groups. For example, in 2003, Macrovision was awarded the Software Industry Award for Best Security Initiative. Macrovision was chosen for its industry-wide leadership in software protection and security throughout its comprehensive portfolio of products.[9] In 2004, the Macrovision FLEXnet licensing platform was awarded the "Best Digital Rights Management Solution" award by the Software & Information Industry Association CODiE Awards.[10] In 2005, Rovi's InstallShield was inducted into the JOLT Product Hall of Fame by Software Development magazine, an honor given to only one product each year. In addition, InstallShield was given the "Riding the Crest" award for the 2004 best-selling installation and deployment tool by Programmer's Paradise.[11]

32. Rovi's history of innovation is also reflected in the extensive patent coverage that Rovi has obtained for its inventions. This portfolio, which includes more than 233 issued patents worldwide, is a direct result of Rovi's substantial and ongoing investment in research and development. The asserted MOV Intelligence patents are reflective of this history of innovation, embodying a number of firsts in the development of DRM and watermarking technologies.

---

[9] MACROVISION WINS 2003 SOFTWARE INDUSTRY AWARD FOR BEST SECURITY INITIATIVE (October 31, 2003) ("Software Business Magazine's Annual Software Industry Awards recognize software companies that have displayed broad leadership with their initiatives and products, distinguishing their brands and strategies from a pool of nominations submitted by many successful software companies.").

[10] SIIA CODIE AWARDS (2004); *available at:* http://www.siia.net/archive/codies/2015/pw_2004.asp.

[11] MACROVISION'S INSTALLSHIELD INDUCTED INTO SOFTWARE DEVELOPMENT MAGAZINE'S JOLT AWARDS HALL OF FAME (March 24, 2005); *available at*: http://www.flexerasoftware.com/producer/company/news-center/press-releases.

33. The strength of MOV Intelligence's patent portfolio has been recognized by the technology industry. In particular, Google, Inc., LG Electronics, Sony Corporation, Sharp Corporation, and Verizon Communications, Inc. among others, have acknowledged the importance of MOV Intelligence's innovations by taking licenses to patents covering the technologies at issue in this case. In addition to selling products and solutions incorporating its innovative technology to various companies, Rovi has received hundreds of millions of dollars in licensing revenue from technology companies who rely on Rovi's DRM and watermarking inventions.

34. MOV Intelligence and ROVI's long-term financial success depends in part on its ability to establish, maintain, and protect its proprietary technology through patents. Defendant's infringement presents significant and ongoing damage to MOV Intelligence and ROVI's business.

35. Defendants, in an effort to expand their product offerings and profit from the sale of ROVI's technology, have chosen to incorporate Macrovision's fundamental technology without a license or payment. The patents MOV Intelligence owns and licenses have been the subject of widespread misappropriation by numerous industry members who have utilized MOV Intelligence's foundational technology as a base around which to build successful products.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,200,230

36. U.S. Patent No. 7,200,230 (the "'230 patent"), entitled "System and Method for Controlling and Enforcing Access Rights to Encrypted Media," was filed January 15, 2001, and claims priority to April 6, 2000. MOV Intelligence is the owner by assignment of the '230 patent. A true and correct copy of the '230 patent is attached hereto as Exhibit A. The '230 patent claims specific methods and systems for extending the capabilities of rights controlled access media systems. Further, the system and methods provide for designation and authentication of the identity of the data processor upon/through which a data object is to be

used. The system and methods also provide\ for encryption of a data object and its associated rules such that only a designated data processor can decrypt and use the data object. The system and methods further provide for designation and authentication of the identity of a user by whom the data object is to be used. The system and methods also provide for encryption of a data object and its associated rules such that only a designated user can decrypt and use the data object.

37. The ‘230 patent has been cited by over 180 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘230 patent as relevant prior art:

- International Business Machines Corporation
- Qualcomm Incorporated
- Autodesk, Inc.
- NTT Docomo, Inc.
- Hitachi, Ltd.
- Koninklijke Phillips Electronics N.C.
- Hewlett-Packard Development Company L.P.
- Time Warner Cable, Inc.
- Cisco Systems, Inc.
- Blackberry Limited
- Arris Enterprises, Inc.
- Meshnetworks, Inc.
- Google, Inc. (now Alphabet, Inc.)
- Oracle Corporation
- General Instrument Corporation
- Symantec Corporation
- Siemens Aktiengesellschaft
- AT&T, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Voltage Security, Inc.
- Scientific-Atlanta, Inc. (subsequently acquired by Cisco Systems, Inc.)
- Telefonaktiebolaget LM Ericsson

38. The ‘230 patent claims a technical solution to a problem unique to the transmission of digital information over a network – providing systems and methods for

extending the capabilities of rights controlled access to digital content using three layers of encryption.

U.S. PATENT NO. 6,802,006

39. U.S. Patent No. 6,802,006 (the "'006 patent"), entitled "System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images," was filed on July 22, 1999, and claims priority to January 15, 1999. MOV Intelligence is the owner by assignment of the '006 patent. A true and correct copy of the '006 patent is attached hereto as Exhibit B. The '006 patent claims specific methods and systems for verifying the authenticity of executable images. The system includes a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified.

40. The '006 patent has been cited by over 85 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '006 patent as relevant prior art:

- Intertrust Technologies Corporation
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Check Point Software Technologies, Inc.
- Nokia Corporation
- Ipass, Inc.
- Nytell Software LLC
- Amazon Technologies, Inc.
- Panasonic Corporation
- Matsushita Electric Ind. Co. Ltd.
- NXP B.V. (now Cisco Systems, Inc.)
- Intel Corporation
- Hewlett-Packard Development Company, L.P.
- Apple, Inc.
- Lockheed Martin Corporation
- Symantec Corporation

- Zone Labs, Inc.

41. The ‘006 patent claims a technical solution to a problem unique to computer systems: verifying and authenticating executable images.

U.S. PATENT NO. 6,510,516

42. U.S. Patent No. 6,510,516 (the “‘516 patent”), entitled “System and Method for Authenticating Peer Components,” was filed on January 15, 1999, and claims priority to January 16, 1998. MOV Intelligence is the owner by assignment of the ‘516 patent. A true and correct copy of the ‘516 patent is attached hereto as Exhibit C. The ‘516 patent claims specific methods and systems for controlling the usage of data objects in component object systems. According to the invention, each data object includes a peer list that defines one or more peer data objects that are required by the data object. Upon receipt of a data object, the system verifies the integrity of the data object. Further, the system identifies the integrity of the peer data objects.

43. The ‘516 patent family has been cited by over 108 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘516 patent as relevant prior art:

- America Online, Inc.
- LG Electronics, Inc.
- Microsoft Corporation
- Samsung Electronics Co., Ltd.
- First Data Corporation
- International Business Machines Corporation
- Pixar, Inc. (now a subsidiary of the Walt Disney Company)
- Adobe Systems Incorporated
- The Western Union Company
- Verizon Communications, Inc.
- JPMorgan Chase & Co.
- Electronics and Telecommunications Research Institute (ETRI)
- Siemens Medical Solutions USA, Inc.

44. The ‘516 patent claims a technical solution to a problem unique to the transmission of digital information over a network: controlling the usage of data in a system having one or more peer data objects.

U.S. PATENT NO. 7,650,504

45. U.S. Patent No. 7,650,504 (the "'504 patent"), entitled "System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images," was filed on August 23, 2004, and claims priority to July 22, 1999. MOV Intelligence is the owner by assignment of the '504 patent. A true and correct copy of the '504 patent is attached hereto as Exhibit D. The '504 patent claims specific methods and systems for verifying the authenticity of executable images. The systems and methods taught in the '504 patent incorporate a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified. In addition, the validator ensures that each of the pointers in the executable image have not been improperly redirected.

46. The '504 patent and its underlying application have been cited by over 30 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '504 patent as relevant prior art:

- Qualcomm Incorporated
- Intel Corporation
- Micro Beef Technologies, Ltd
- Microsoft Corporation
- Apple, Inc.
- Symantec Corporation
- Samsung Electronics Co., Ltd.
- Cybersoft Technologies, Inc.
- Electronics and Telecommunications Research Institute (ETRI)

47. The '504 patent claims a technical solution to a problem unique to the transmission of digital information over a network: verifying the identity of a software application in a dynamic loading environment. In particular, the system determines whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

U.S. PATENT NO. 7,124,114

48. U.S. Patent No. 7,124,114 (the "'114 patent"), entitled "Method and Apparatus for Determining Digital A/V Content Distribution Terms Based on Detected Piracy Levels," was filed on November 9, 2000. MOV Intelligence is the owner by assignment of the '114 patent. A true and correct copy of the '114 patent is attached hereto as Exhibit E. The '114 patent claims specific methods and systems for distributing copyrighted material over a computer network. Specifically, the '114 patent teaches the providing of protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient; and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms. The '114 patent also discloses the use of a first set of program code which serves to ascertain terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient. The first set of program code also serves to provide or withhold a copy of the protected material to or from the prospective recipient in accordance with the terms.

49. The '114 patent family has been cited by over 39 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '114 patent as relevant prior art:

- Google, Inc.
- NBCUniversal Media, Inc.
- Digimarc Corporation
- Hewlett-Packard Development Company, L.P.
- Aigo Research Institute of Image Computing Co., Ltd.
- AT&T Intellectual Property I, L.P.
- General Electric Company
- The Nielsen Company (US), LLC
- Sca Ipla Holdings, Inc.
- Thomson Licensing, Inc.
- Fujitsu Limited

50. The '114 patent claims a technical solution to a problem unique to the transmission of digital information over a network: preventing the unauthorized copying of

digital content. The patent teaches the use of a distribution server that distributes A/V content to a recipient according to terms determined from information stored in a database of prior unauthorized copying attributed to that recipient. The copy distributed to the recipient includes identifications of the content and recipient embedded in it by an ID embedder.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,200,230

51. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

52. Fujitsu designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for digital rights management.

53. Fujitsu designs, makes, sells, offers to sell, imports, and/or uses Marlin Embedded DRM middleware, including the Inspirium DRM library/server for Marlin and DRM middleware conforming to Marlin IPTV-ES, and the Marlin ASP service, including the Fujitsu ASP service for DRM server conforming to Marlin IPTV-ES (the "Fujitsu '230 Product(s)").

54. On information and belief, one or more Fujitsu subsidiaries and/or affiliates use the Fujitsu '230 Products in regular business operations.

55. On information and belief, one or more of the Fujitsu '230 Products include digital rights management technology.

56. On information and belief, one or more of the Fujitsu '230 Products enable associating a user program key with a user program configured to run on a user data processor.

57. On information and belief, the Fujitsu '230 Products are available to businesses and individuals throughout the United States.

58. On information and belief, the Fujitsu '230 Products are provided to businesses and individuals located in the Eastern District of Texas.

59. On information and belief, the Fujitsu ‘230 Products enable determining whether the use of the data object is to be restricted to a particular user data processor.

60. On information and belief, the Fujitsu ‘230 Products comprise a system wherein a machine key device is associated with the particular user data processor. Further, the machine key device is accessible by the user program, and the machine key device maintains a portion of a machine key.

61. On information and belief, the Fujitsu ‘230 Products enable encrypting a data object so the decryption of a first secure layer and a second secure layer of the encrypted data object requires the user program key and the machine key.

62. On information and belief, the Fujitsu ‘230 Products enable determining whether the use of the data object is to be restricted to a particular user.

63. On information and belief, the Fujitsu ‘230 Products provide for the designation and authentication of the identity of a user by whom the data object is to be used.

64. On information and belief, the Fujitsu ‘230 Products enable associating a user key device with the particular user. Further, the Fujitsu ‘230 Products enable the user key device to be made accessible by the user program. And, the user key device maintains a portion of a user key.

65. On information and belief, the Fujitsu ‘230 Products contain functionality for encrypting a data object so the decryption of a third secure layer of the encrypted data object requires the user key.

66. On information and belief, the Fujitsu ‘230 Products contain functionality wherein the third key used by the system for managing digital rights is the media access controller (MAC) address of the user data processor.

67. On information and belief, the Fujitsu ‘230 Products provide for encryption of a data object so only a designated data processor can decrypt and use the data object.

68. On information and belief, the Fujitsu ‘230 Products enable user specific digital rights management authorization and access.

69. On information and belief, Fujitsu has directly infringed and continues to directly infringe the ‘230 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Fujitsu ‘230 Products, which include infringing digital rights management technology. Such products and/or services include, by way of example and without limitation, the Marlin Embedded DRM middleware, including the Inspirium DRM library/server for Marlin and DRM middleware conforming to Marlin IPTV-ES, and the Marlin ASP service, including the Fujitsu ASP service for DRM server conforming to Marlin IPTV-ES.

70. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Fujitsu ‘230 Products, Fujitsu has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘230 patent, including at least claim 39, pursuant to 35 U.S.C. § 271(a).

71. On information and belief, Fujitsu also indirectly infringes the ‘230 patent by actively inducing infringement under 35 USC § 271(b).

72. On information and belief, Fujitsu had knowledge of the ‘230 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Fujitsu knew of the ‘230 patent and knew of its infringement, including by way of this lawsuit.

73. On information and belief, Fujitsu intended to induce patent infringement by third-party customers and users of the Fujitsu ‘230 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Fujitsu specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘230 patent. Fujitsu performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘230 patent and with the knowledge that the induced acts would constitute infringement. For example, Fujitsu provides the Fujitsu ‘230 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘230 patent, including at least claim 39, and

Fujitsu further provides documentation and training materials that cause customers and end users of the Fujitsu '230 Products to utilize the products in a manner that directly infringe one or more claims of the '230 patent. By providing instruction and training to customers and end-users on how to use the Fujitsu '230 Products in a manner that directly infringes one or more claims of the '230 patent, including at least claim 39, Fujitsu specifically intended to induce infringement of the '230 patent. On information and belief, Fujitsu engaged in such inducement to promote the sales of the Fujitsu '230 Products, e.g., through Fujitsu user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '230 patent. Accordingly, Fujitsu has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '230 patent, knowing that such use constitutes infringement of the '230 patent.

74. The '230 patent is well-known within the industry as demonstrated by the over 180 citations to the '230 patent family in published patents and published patent applications assigned to technology companies and academic institutions. Several of Fujitsu's competitors have paid considerable licensing fees for their use of the technology claimed by the '230 patent. In an effort to gain an advantage over Fujitsu's competitors by utilizing the same licensed technology without paying reasonable royalties, Fujitsu infringed the '230 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

75. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '230 patent.

76. As a result of Fujitsu's infringement of the '230 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Fujitsu's infringement, but in no event less than a reasonable royalty for the use made of the invention by Fujitsu together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,802,006

77. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

78. Fujitsu designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for determining the authenticity of an executable image.

79. Fujitsu designs, makes, sells, offers to sell, imports, and/or uses the ETERNUS Storage Systems Monitoring system, including the Fujitsu Eternus Storage Systems Monitoring Pack version 16.0, version PRO 16.0, and version 16.3 (the "Fujitsu '006 Product(s)").

80. On information and belief, one or more Fujitsu subsidiaries and/or affiliates use the Fujitsu '006 Products in regular business operations.

81. On information and belief, one or more of the Fujitsu '006 Products include authentication technology.

82. On information and belief, one or more of the Fujitsu '006 Products enable authenticating the identity of a software application in a dynamic loading environment. In particular, the Fujitsu '006 Products determine whether an executable image has been dynamically connected to another data object that has been tampered with subsequent to the execution of the software application.

83. On information and belief, the Fujitsu '006 Products are available to businesses and individuals throughout the United States.

84. On information and belief, the Fujitsu '006 Products are provided to businesses and individuals located in the Eastern District of Texas.

85. On information and belief, the Fujitsu '006 Products enable identifying one or more locations within the executable image, each of the identified locations being modified by a program loader.

86. On information and belief, the Fujitsu '006 Products comprise a system wherein a reference digital signature is generated based on an executable image.

87. On information and belief, the Fujitsu ‘006 Products generate a reference digital signature that excludes one or more locations in an executable image.

88. On information and belief, the Fujitsu ‘006 Products are capable of storing the reference digital signature on a computer network.

89. On information and belief, the Fujitsu ‘006 Products comprise systems and methods wherein an authenticity digital signature is generated based on an executable image.

90. On information and belief, the Fujitsu ‘006 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

91. On information and belief, the Fujitsu ‘006 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

92. On information and belief, the Fujitsu ‘006 Products contain functionality that generates a warning if the reference digital signature does not match the authenticity digital signature.

93. On information and belief, the Fujitsu ‘006 Products contain functionality wherein the digital signature is generated based on a first and second point in time. For example, one or more of the Fujitsu ‘006 Products generate a reference digital signature at a first point in time. Subsequently, an authenticity digital signature is generated (at a second point in time).

94. On information and belief, the Fujitsu ‘006 Products comprise a system and method that generates a digital signature based on a hash value. Specifically, the reference digital signature that is generated by the Fujitsu ‘006 Products at a first point in time is based on a hash value. Later the authenticity digital signature is also generated based on a hash function that is used to check data integrity.

95. On information and belief, the Fujitsu ‘006 Products comprise a system and method that can verify the identity a computer application.

96. On information and belief, the Fujitsu ‘006 Products enable the detection of corrupted data in a computer image.

97. On information and belief, the Fujitsu ‘006 Products enable the verification of the integrity of software images.

98. On information and belief, Fujitsu has directly infringed and continues to directly infringe the ‘006 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Fujitsu ‘006 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the ETERNUS Storage Systems Monitoring system, including the Fujitsu Eternus Storage Systems Monitoring Pack version 16.0, version PRO 16.0, and version 16.3.

99. By making, using, testing, offering for sale, and/or selling verification and authentication products and services, including but not limited to the Fujitsu ‘006 Products, Fujitsu has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, pursuant to 35 U.S.C. § 271(a).

100. On information and belief, Fujitsu also indirectly infringes the ‘006 patent by actively inducing infringement under 35 USC § 271(b).

101. On information and belief, Fujitsu had knowledge of the ‘006 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Fujitsu knew of the ‘006 patent and knew of its infringement, including by way of this lawsuit.

102. On information and belief, Fujitsu intended to induce patent infringement by third-party customers and users of the Fujitsu ‘006 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Fujitsu specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘006 patent. Fujitsu performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge

of the ‘006 patent and with the knowledge that the induced acts would constitute infringement. For example, Fujitsu provides the Fujitsu ‘006 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, and Fujitsu further provides documentation and training materials that cause customers and end users of the Fujitsu ‘006 Products to utilize the products in a manner that directly infringe one or more claims of the ‘006 patent. By providing instruction and training to customers and end-users on how to use the Fujitsu ‘006 Products in a manner that directly infringes one or more claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, Fujitsu specifically intended to induce infringement of the ‘006 patent. On information and belief, Fujitsu engaged in such inducement to promote the sales of the Fujitsu ‘006 Products, *e.g.*, through Fujitsu user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘006 patent. Accordingly, Fujitsu has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘006 patent, knowing that such use constitutes infringement of the ‘006 patent.

103. The ‘006 patent is well-known within the industry as demonstrated by the over 85 citations to the ‘006 patent in issued patents and published patent applications assigned to technology companies and academic institutions. Several of Fujitsu’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘006 patent. In an effort to gain an advantage over Fujitsu’s competitors by utilizing the same licensed technology without paying reasonable royalties, Fujitsu infringed the ‘006 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

104. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘006 patent.

105. As a result of Fujitsu’s infringement of the '006 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for

Fujitsu's infringement, but in no event less than a reasonable royalty for the use made of the invention by Fujitsu together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 6,510,516

106. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

107. Defendants, in a joint enterprise, design, make, use, sell, and/or offer for sale in the United States products and/or services for authenticating peer data objects.

108. Defendants, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the PRIMEFLEX for SAP HANA and PRIMEFLEX for SAP Landscapes (the "Defendants' '516 Product(s)") pursuant to ongoing contractual agreements between Defendants.

109. On information and belief, one or more of Defendants' subsidiaries and/or affiliates use the Defendants' '516 Products in regular business operations.

110. On information and belief, one or more of the Defendants' '516 Products include authentication technology.

111. On information and belief, one or more of the Defendants' '516 Products enable authenticating the identity of peer data objects.

112. On information and belief, the Defendants' '516 Products are available to businesses and individuals throughout the United States.

113. On information and belief, the Defendants' '516 Products are provided to businesses and individuals located in the Eastern District of Texas.

114. On information and belief, the Defendants' '516 Products enable first data objects to contain or be linked to a description of one or more peer data objects that are required to be connected to the first data object before the data object can be accessed by the peer data objects.

115. On information and belief, the Defendants' '516 Products enable the use of a digital signature that identifies the provider of a data object.

116. On information and belief, the Defendants' '516 Products contain systems and methods that comprise reading from a data object a description of one or more peer data objects that is required for use of the data object.

117. On information and belief, the Defendants' '516 Products contain functionality for determining whether the data object is authorized to communicate with one or more peer data objects.

118. On information and belief, the Defendants' '516 Products contain the capability to determine if the data object is authorized to communicate with one or more peer data objects.

119. On information and belief, the Defendants' '516 Products are capable of controlling the connection of the peer data objects to the data object.

120. On information and belief, the Defendants' '516 Products comprise systems and methods that connect a data object to peer data objects based upon authorization being granted. Moreover, when authorization is granted for the connection of a data object to peer data objects the peer data objects can communicate with the data object and the data object can communicate with the peer data objects.

121. On information and belief, the Defendants' '516 Products support authenticating a data object where the data object is encrypted.

122. On information and belief, Defendants have directly infringed and continues to directly infringe the '516 patent by, among other things, making, using, offering for sale, and/or selling data object authentication and verification technology, including but not limited to the Defendants' '516 Products, which include infringing verification and authentication technologies. Such products and/or services include, by way of example and without limitation, the PRIMEFLEX for SAP HANA and PRIMEFLEX for SAP Landscapes.

123. By making, using, testing, offering for sale, and/or selling authentication and verification products and services, including but not limited to the Defendants' '516 Products,

Defendants, acting as a joint enterprise and pursuant to ongoing contractual agreements, have injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '516 patent, including at least claims 1, 17, and 20, pursuant to 35 U.S.C. § 271(a).

124. On information and belief, Defendants also indirectly infringe the '516 patent by actively inducing infringement under 35 USC § 271(b).

125. On information and belief, Defendants had knowledge of the '516 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Defendants knew of the '516 patent and knew of its infringement, including by way of this lawsuit.

126. On information and belief, Defendants intended to induce patent infringement by third-party customers and users of the Defendants' '516 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Defendants specifically intended and was aware that the normal and customary use of the accused products would infringe the '516 patent. Defendants performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '516 patent and with the knowledge that the induced acts would constitute infringement. For example, Defendants provide the Defendants' '516 Products that have the capability of operating in a manner that infringe one or more of the claims of the '516 patent, including at least claims 1, 17, and 20, and Defendants further provide documentation and training materials that cause customers and end users of the Defendants' '516 Products to utilize the products in a manner that directly infringe one or more claims of the '516 patent. By providing instruction and training to customers and end-users on how to use the Defendants' '516 Products in a manner that directly infringes one or more claims of the '516 patent, including at least claims 1, 17, and 20, Defendants specifically intended to induce infringement of the '516 patent. On information and belief, Defendants engaged in such inducement to promote the sales of the Defendants' '516 Products, e.g., through Defendants' user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '516 patent. Accordingly, Defendants have induced and continues to induce users

of the accused products to use the accused products in their ordinary and customary way to infringe the ‘516 patent, knowing that such use constitutes infringement of the ‘516 patent.

127. The ‘516 patent is well-known within the industry as demonstrated by the over 108 citations to the ‘516 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, LG Electronics, Inc. and Siemens AG). Several of Defendants’ competitors have paid considerable licensing fees for their use of the technology claimed by the ‘516 patent. In an effort to gain an advantage over Defendants’ competitors by utilizing the same licensed technology without paying reasonable royalties, Defendants infringed the ‘516 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

128. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘516 patent.

129. As a result of Defendants’ infringement of the '516 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Defendants’ infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,650,504

130. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

131. Fujitsu designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for verifying the authenticity of executable images.

132. Fujitsu designs, makes, sells, offers to sell, imports, and/or uses the ETERNUS Storage Systems Monitoring system, including the Fujitsu Eternus Storage Systems Monitoring Pack version 16.0, version PRO 16.0, and version 16.3 (the “Fujitsu ‘504 Product(s)”).

133. On information and belief, one or more Fujitsu subsidiaries and/or affiliates use the Fujitsu '504 Products in regular business operations.

134. On information and belief, one or more of the Fujitsu '504 Products include authentication technology.

135. On information and belief, one or more of the Fujitsu '504 Products comprise systems and methods for determining the authenticity of an executable image.

136. On information and belief, one or more of the Fujitsu '504 Products enable authenticating and verifying an executable image. In particular, the Fujitsu '504 Products determine whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

137. On information and belief, the Fujitsu '504 Products are available to businesses and individuals throughout the United States.

138. On information and belief, the Fujitsu '504 Products are provided to businesses and individuals located in the Eastern District of Texas.

139. On information and belief, the Fujitsu '504 Products enable the use of a reference digital signature for an executable image. The reference digital signature uses the contents of the executable image excluding portions of the executable that are fixed-up by a program loader.

140. On information and belief, the Fujitsu '504 Products comprise a system wherein a reference digital signature is generated based on an executable image.

141. On information and belief, the Fujitsu '504 Products generate a reference digital signature that excludes one or more locations in an executable image.

142. On information and belief, the Fujitsu '504 Products comprise systems and methods wherein subsequent to the loading of the executable image the '504 Products determine an authenticity digital signature to verify that the executable image has not been improperly modified.

143. On information and belief, the Fujitsu '504 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

144. On information and belief, the Fujitsu '504 Products are systems and methods that generate an authenticity digital signature after the executable image is loaded into memory. The authenticity digital signature which is generated by the Fujitsu '504 Products excludes one or more pointers in need of fixing up;

145. On information and belief, the Fujitsu '504 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

146. On information and belief, the Fujitsu '504 Products enable the generating of a reference digital signature prior to loading the executable image into memory. Specifically, the Fujitsu '504 Products generate a reference digital signature that excludes one or more pointers from the reference digital signature.

147. On information and belief, the Fujitsu '504 Products contain functionality wherein the digital signature is generated based on a first and second point in time.

148. On information and belief, the Fujitsu '504 Products have the ability to compare the reference digital signature and the authenticity digital signature to perform an authenticity check.

149. On information and belief, the Fujitsu '504 Products enable the detection of corrupted data in a computer image.

150. On information and belief, the Fujitsu '504 Products enable the verification of the integrity of software images.

151. On information and belief, Fujitsu has directly infringed and continues to directly infringe the '504 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Fujitsu '504 Products, which includes technology for verifying the authenticity of a software image. Such products and/or

services include, by way of example and without limitation, the ETERNUS Storage Systems Monitoring system, including the Fujitsu Eternus Storage Systems Monitoring Pack version 16.0, version PRO 16.0, and version 16.3.

152. By making, using, testing, offering for sale, and/or selling authentication and verification technologies and services, including but not limited to the Fujitsu '504 Products, Fujitsu has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '504 patent, including at least claims 1 and 10, pursuant to 35 U.S.C. § 271(a).

153. On information and belief, Fujitsu also indirectly infringes the '504 patent by actively inducing infringement under 35 USC § 271(b).

154. On information and belief, Fujitsu had knowledge of the '504 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Fujitsu knew of the '504 patent and knew of its infringement, including by way of this lawsuit.

155. On information and belief, Fujitsu intended to induce patent infringement by third-party customers and users of the Fujitsu '504 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Fujitsu specifically intended and was aware that the normal and customary use of the accused products would infringe the '504 patent. Fujitsu performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '504 patent and with the knowledge that the induced acts would constitute infringement. For example, Fujitsu provides the Fujitsu '504 Products that have the capability of operating in a manner that infringe one or more of the claims of the '504 patent, including at least claims 1 and 10, and Fujitsu further provides documentation and training materials that cause customers and end users of the Fujitsu '504 Products to utilize the products in a manner that directly infringe one or more claims of the '504 patent. By providing instruction and training to customers and end-users on how to use the Fujitsu '504 Products in a manner that directly infringes one or more claims of the '504 patent, including at least claims 1 and 10, Fujitsu specifically intended to

induce infringement of the ‘504 patent. On information and belief, Fujitsu engaged in such inducement to promote the sales of the Fujitsu ‘504 Products, e.g., through Fujitsu user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘504 patent. Accordingly, Fujitsu has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘504 patent, knowing that such use constitutes infringement of the ‘504 patent.

156. The ‘504 patent is well-known within the industry as demonstrated by the over 30 citations to the ‘504 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Apple, Inc. and Electronics and Telecommunications Research Institute (ETRI)). Several of Fujitsu’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘504 patent. In an effort to gain an advantage over Fujitsu’s competitors by utilizing the same licensed technology without paying reasonable royalties, Fujitsu infringed the ‘504 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

157. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘504 patent.

158. As a result of Fujitsu’s infringement of the '504 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Fujitsu’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fujitsu together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 7,124,114

159. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

160. Fujitsu designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

161. Fujitsu designs, makes, sells, offers to sell, imports, and/or uses the Fujitsu SuperView Resource Orchestrator v3.1 DR Option, v3.1 Cloud Edition, and v3.1 Virtual Edition (the "Fujitsu '114 Product(s)").

162. On information and belief, one or more Fujitsu subsidiaries and/or affiliates use the Fujitsu '114 Products in regular business operations.

163. On information and belief, one or more of the Fujitsu '114 Products include content protection and content access technology.

164. On information and belief, one or more of the Fujitsu '114 Products enable providing or withholding access to digital content is accordance with digital rights management protection terms.

165. On information and belief, the Fujitsu '114 Products are available to businesses and individuals throughout the United States.

166. On information and belief, the Fujitsu '114 Products are provided to businesses and individuals located in the Eastern District of Texas.

167. On information and belief, the Fujitsu '114 Products enable the distribution of protected digital data.

168. On information and belief, the Fujitsu '114 Products comprise systems and methods wherein the Fujitsu '114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

169. On information and belief, the Fujitsu '114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms.

170. On information and belief, Fujitsu has directly infringed and continues to directly infringe the ‘114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Fujitsu ‘114 Products, which include infringing digital rights management technologies. Such products and/or services include, by way of example and without limitation, the Fujitsu SuperView Resource Orchestrator v3.1 DR Option, v3.1 Cloud Edition, and v3.1 Virtual Edition.

171. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the Fujitsu ‘114 Products, Fujitsu has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, pursuant to 35 U.S.C. § 271(a).

172. On information and belief, Fujitsu also indirectly infringes the ‘114 patent by actively inducing infringement under 35 USC § 271(b).

173. On information and belief, Fujitsu had knowledge of the ‘114 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Fujitsu knew of the ‘114 patent and knew of its infringement, including by way of this lawsuit.

174. On information and belief, Fujitsu intended to induce patent infringement by third-party customers and users of the Fujitsu ‘114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Fujitsu specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘114 patent. Fujitsu performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘114 patent and with the knowledge that the induced acts would constitute infringement. For example, Fujitsu provides the Fujitsu ‘114 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, and Fujitsu further provides documentation and training materials that cause customers and end users of the Fujitsu ‘114 Products to utilize the products in a manner that

directly infringe one or more claims of the ‘114 patent. By providing instruction and training to customers and end-users on how to use the Fujitsu ‘114 Products in a manner that directly infringes one or more claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, Fujitsu specifically intended to induce infringement of the ‘114 patent. On information and belief, Fujitsu engaged in such inducement to promote the sales of the Fujitsu ‘114 Products, e.g., through Fujitsu user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘114 patent. Accordingly, Fujitsu has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘114 patent, knowing that such use constitutes infringement of the ‘114 patent.

175. The ‘114 patent is well-known within the industry as demonstrated by the over 39 citations to the ‘114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image Computing Co., Ltd. and General Electric Company). Several of Fujitsu’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘114 patent. In an effort to gain an advantage over Fujitsu’s competitors by utilizing the same licensed technology without paying reasonable royalties, Fujitsu infringed the ‘114 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

176. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘114 patent.

177. As a result of Fujitsu’s infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Fujitsu’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fujitsu together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff MOV Intelligence respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff MOV Intelligence that Fujitsu has infringed, either literally and/or under the doctrine of equivalents, the '230 patent; the '006 patent; the '504 patent; and the '114 patent;

B. A judgment in favor of Plaintiff MOV Intelligence that Fujitsu and SAP have jointly infringed in a joint enterprise and pursuant to ongoing contractual agreements between Fujitsu and SAP, either literally and/or under the doctrine of equivalents, the '516 patent;

C. An award of damages resulting from Defendants' acts of infringement in accordance with 35 U.S.C. § 284;

D. A judgment and order finding that Defendants' infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

E. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendants.

F. Any and all other relief to which MOV Intelligence may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, MOV Intelligence requests a trial by jury of any issues so triable by right.

Dated: September 23, 2016

Respectfully submitted,

/s/ Dorian S. Berger

Elizabeth L. DeRieux (TX Bar No. 05770585)
D. Jeffrey Rambin (TX Bar No. 00791478)
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 95047
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Attorneys for Marking Object Virtualization Intelligence, LLC